2021 年 11 月 30 日

一般社団法人 JPCERT コーディネーションセンター

CSIRT マテリアルの改訂版の公開にあたって

1　CSIRT マテリアルについて

CSIRT マテリアル（以下「本マテリアル」）は、一般社団法人 JPCERT コーディネーションセンターが平成 18 年度に実施した、企業等の組織内における CSIRT（Computer Security Incident Response Team）機能の構築を支援する一連の活動の成果物として初版を公開しました。

組織の事業内容や規模、部門構成、業務遂行形態、それぞれの組織や事業に対応する脅威やリスクの定義により、それぞれの組織内 CSIRT の活動内容や形態などが大きく異なるため、組織の状況にあわせて機能を構築していただくことが組織内 CSIRT を有効に機能させるうえで重要な意味を持ちます。本マテリアルは、これから組織内 CSIRT を構築しようとする組織だけではなく、すでに組織内 CSIRT やそれに準ずる組織を擁する組織に対しても、自社の CSIRT の運用を振り返るための機会を提供することを目的としています。

本マテリアルは初版の公開後も IT セキュリティ脅威の変化を踏まえて、CSIRT 構築にあたる普遍的な部分を大切にしながら加筆・修正を行っています。このたびの改訂では、CSIRT の体制整備と運用、インシデント対応に関する現在の知見をもとに加筆修正するとともに、PSIRT に代表される組織の提供物に対するセキュリティの取り組みといった組織のセキュリティ対応のスコープの変化を記述内容に反映し、さらにインシデント対応演習の実施について詳説する参考資料を新たに加えています。また旧版の資料中で紹介していた古いインシデント事例の一部を新しいものに入れ替え、旧版では多数の文書に分かれて記述されていたものを可能な限りまとめるなど、資料の使いやすさの改善を図っています。

2　背景

最近の情報セキュリティ上の脅威の動向として、従来の不特定多数を狙った愉快犯と見られる攻撃が目立たなくなる一方で、特定の企業や組織を狙った攻撃が高度化していることが指摘されています。特に、経済的利得の不正取得などの明確な目的に基づいた標的型攻撃が増加するとともに、その攻撃手法が巧妙化・不可視化するなど、情報資産への脅威は増大しているといえます。また、脅威やリスクのとらえ方が企業・組織ごとに異なることもあり、想定される事前対策の内容もさまざまです。

そのため、個々の企業・組織に最適な情報セキュリティ管理体制や情報セキュリティ施策を組織全体に運用して、リスク管理の枠組みのなかで個々の事象に適切に対応するのは容易ではありません。

また、事業活動がかつてないほどにIT（情報技術）の利活用を前提とし、システムやネットワークの相互依存関係が無視できなくなってきている現況にかんがみると、システムやネットワーク上で発生したコンピューターセキュリティインシデント[1]（以下「インシデント」という。）の潜在的影響と被害は、従来の予測を超える規模に達することが予想されます。さらに、広範な企業・組織に対して功を奏する攻撃手法によるインシデント（ボットネット、フィッシング、高度サイバー攻撃(APT)等）の問題も広がりを見せており[2]、組織を超えたインシデント対応の連携が求められる状況が発生しています。

このような状況から、情報資産保護策の一環として、考えられるあらゆる攻撃に対応する部門または部門を横断した対応チームを設け、組織内にインシデント対応機能を持つ必要性が高まってきています。組織内CSIRTとは、このようなチーム・機能のことをいいます。組織内CSIRTを設けて、従来組織内に点在していたインシデントに関する情報を集約することにより、インシデントが発生した際に迅速かつ的確な「組織としての意思決定と対応」を行うことが可能となり、被害の最小化および同様の問題に対する事前策の検討などの効果を期待することができるようになります[3]。
また、組織内CSIRTが外部のインシデント対応組織等との情報共有や信頼関係の構築の役割を担うことにより、組織外に起因するインシデントが発生した際に、そのインシデントに直接対応できる組織への対応依頼等を円滑に進めることができ、早期の解決を図ることができるようになります。

このように、組織内にCSIRT機能を実現するための体制を構築し、組織としてのインシデント対応能力を向上させることの意義は大きく、情報セキュリティ管理体制の強化のみならず組織基盤の強化にも寄与する取り組みであるといえます。

3　本マテリアルの目的

各組織において組織内CSIRTを構築する必要性が認識された後は、経営層の理解と意思決定を端緒として組織内CSIRTの構築に着手するのが一般的です。その際には、提案者とITリスク管理に関係する各部門やITユーザーとの連携が不可欠となります。
組織内にCSIRTを構築する必要性が理解された後に問題となるのは、構築に必要となる情

[1] コンピューターセキュリティインシデントの定義は組織ごとに異なるが、一例としてJPCERTコーディネーションセンターの定義（https://www.jpcert.or.jp/aboutincident.html）では「情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象」としている。
[2] ボットネットの現況については、JPCERTコーディネーションセンターが2006年7月に公開した調査報告書「ボットネットの概要」を参照されたい（https://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf）。APTとは先進的で（Advanced）執拗な（Persistent）脅威（Threat）。
[3] 組織内CSIRTの位置づけや主要な役割期待の定義例については、本活動成果物の各マテリアルを参照されたい。

報が十分に得られないという問題です。組織内 CSIRT の構築に向けた取り組みは海外で先行して開始されたため、過去においては、関連する情報を積極的に入手するためには海外文献に頼らざるを得ませんでした[4]。
また、組織内に CSIRT を構築することを決定した後に、具体的にどのようなプロセスで構築していくのかを決定するのは容易とはいえません。

本マテリアルは、このような現状にかんがみ、組織内 CSIRT を構築しようとする企画発案や構築にたずさわる方々に、必要な情報の提供と具体的な構築プロセスの立案の支援を行うことを目的として作成しました。インシデント対応の経験のある方が、自組織の既存の体制を整理したり、見直したりして CSIRT の構築に繋げるための参考として頂くことを意図しています。一連の資料では組織内 CSIRT が一般的に備えるべき機能や能力について説明していますが、すべての組織内 CSIRT がそれらを達成しなければならないというものではありません。それぞれの組織の状況に応じた適切な CSIRT の形があり、本資料がそれを見つける際の助けとなれば幸いです。
作成にあたっては、組織内 CSIRT 構築を目指す方々が、本マテリアルを活用して、関係部署や経営層などに対して組織内 CSIRT に関する説明と意識の共通化を進めることができるよう、できるだけ多くの図表を挿入して視覚的に理解いただけるものとなるよう配慮しました。

4　本マテリアルの構成

本マテリアルは、大きく分けて、「組織内 CSIRT の理解」、「組織内 CSIRT 構築の実践」の２つに分類されます。
「組織内 CSIRT の理解」では、組織内 CSIRT の必要性に関する論点として、インシデント対応体制の設置の意義やメリットおよび事前のインシデント対応計画の立案の重要性を説明しています。また組織内 CSIRT の役割モデルを客観的な視点からまとめ、組織の視点から見いだされる組織内 CSIRT の活動の定義と範囲に関する考察ポイント、さらに、組織内 CSIRT の形態分類とそれらの特徴に関する情報を提供しています。これらにより、本マテリアルの利用者に、組織内 CSIRT の必要性に対する理解を深め、自組織に組織内 CSIRT を構築する際の計画立案に役立つポイントを把握していただくことを意図しています。
「組織内 CSIRT の実践」は、組織内 CSIRT 構築の全体的なプロセスに関する情報と実作業に有益な情報を提供しています。また、組織内 CSIRT 構築の実作業をすすめる上で参考に

[4] CERT/CC が公開している CSIRT 構築のための手引き *Handbook for CSIRTs* の日本語訳を JPCERT/CC が「コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック」として提供している（https://www.jpcert.or.jp/research/）。また、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）などが公開した情報セキュリティに関する文書の日本語訳を情報処理推進機構 セキュリティセンター（IPA/ISEC）が提供しているのであわせて参照されたい（https://www.ipa.go.jp/security/publications/nist/index.html）。

し、ひな型として活用できるフォームとその作成例を提供しています。
さらに、平成 18 年度に実施したフィールドリサーチの過程でいただいた要望などを参考に、インシデント対応マニュアルの作成や組織内 CSIRT における情報管理、組織のインシデント担当能力を検証する演習の実施等に役立つ参考資料も提供しています。これらのマテリアルを活用することにより、組織内 CSIRT 構築に必要な人員の割り当てや工数の見積もり等の計画に役立てていただくとともに、実際の構築の作業を円滑に進め、実効的な組織内 CSIRT を運用する一助としていただくことを意図しています。

5　本マテリアルの活用方法

本マテリアルは、下記のように利用することができます。

(1)「組織内 CSIRT の理解」のマテリアルについて

- 利用者自身が、組織内 CSIRT を理解および習得するために通読する。
- 関係部署や経営層に対して組織内 CSIRT への理解を促すために、本マテリアルの全部あるいは一部を説明資料として活用する。

(2)「組織内 CSIRT 構築の実践」のマテリアルについて

- 利用者自身が、組織内 CSIRT の構築に必要な作業の見積もりを算出するために通読する。
- 組織内 CSIRT の構築の実作業の各工程の成果物について、それぞれ提供されている作成例を参考にしながらフォームの各項目を記述することにより、実作業の進捗を進める。また、各成果物の完成をマイルストーンとして、実作業の確実な作業進捗を図る。

(3) 「参考資料」の分類のマテリアルについて

- 利用者自身が、組織内 CSIRT の運用に関して標準的な目安となる情報を把握するために通読する。
- 関係者や経営層に対して、組織内 CSIRT の運用に関して必要な情報を提供するために、本マテリアルの全部あるいは一部を説明資料として活用する。

6　各文書の名称と概要

分類	マテリアル名	概　要
組織内 CSIRT の理解	組織内 CSIRT の理解	・組織内 CSIRT の意義やメリット、事前の対応計画の立案の説明 ・組織内 CSIRT の 3 つの類型とそれぞれの責務と使命の説明 ・インシデントの定義に関する説明と、そのほかに必要となる定義対象の考察点の紹介 ・組織内 CSIRT 要員に必要なスキルの説明と、ヒューマンスキルとテクニカルスキルの両面で求められる要求事項に関する情報、トレーニングに関する情報の説明 ・組織内 CSIRT の設立形態の分類とそれらの特徴の説明

分類	マテリアル名	概　要
組織内 CSIRT 構築の実践	組織内 CSIRT 構築の実践	・組織内 CSIRT の構築に必要な 8 つのプロセスとそれぞれのポイントの説明 ・組織内 CSIRT 構築に必要な実作業の工程の説明
	組織内 CSIRT 構築：構築活動のためのプロジェクト憲章	「組織内 CSIRT 構築の実作業」中の「キックオフ、スケジューリング」における成果物のフォームと作成例
	組織内 CSIRT 構築：構築活動のためのスコープ記述書	「組織内 CSIRT 構築の実作業」中の「ゴールの設定とタスクの細分化」における成果物のフォームと作成例
	組織内 CSIRT 構築：構築に必要な現状把握	「組織内 CSIRT 構築の実作業」中の「組織内の現状把握」における成果物のフォームと作成例
	組織内 CSIRT 構築：CSIRT の基本的な枠組み	「組織内 CSIRT 構築の実作業」中の「組織内 CSIRT の設定」における成果物のフォームと作成例。特に、大きな指針をまとめるときに活用することができる。

	組織内 CSIRT 構築：CSIRT 記述書	「組織内 CSIRT 構築の実作業」中の「組織内 CSIRT の設定」における成果物のフォームと作成例。特に、RFC 2350「コンピュータセキュリティインシデント対応への期待」に準拠するために活用することができる。

分類	マテリアル名	概　要
参考資料	インシデント対応マニュアルの作成について	・インシデント対応マニュアルの作成に必要なノウハウと考察すべきポイントを説明 ・インシデントフローの捉え方の例を提供
	組織内 CSIRT の情報管理と設備について	組織内 CSIRT における情報管理とそれを実装する設備等を整備するために必要な考察および留意ポイントについての説明
	組織内 CSIRT における電話対応について	組織内 CSIRT における電話対応について、配慮すべき事項と、電話応対の記録や要領手順の例を提供
	PGP の説明に役立つデータ	CSIRT 間での連絡に必要になることが多い PGP についての説明に役立つデータを提供
	インシデント対応演習プログラム	CSIRT および組織全体でのインシデント対応能力を検証するための演習の実施についての考え方や手法、サンプルシナリオ等を提供

7　本文書を含む活動成果物の引用・転用について

8　免責事項

9　謝辞

本マテリアル改定版の作成にあたっては、日本シーサート協議会教育コンテンツサブタスクフォースの方々にご協力をいただきました。ここに心より感謝の意を表します。

10　変更履歴

初　版：2007 年 6 月 14 日

第 2 版：2015 年 11 月 19 日

第 2.1 版：2021 年 11 月 30 日

11　連絡先

一般社団法人 JPCERT コーディネーションセンター

Email: pr@jpcert.or.jp